STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

TOWARDS A NATIONAL STRATEGY FOR INFORMATION TECHNOLOGY

BY

LIEUTENANT COLONEL EMANUEL HAMPTON
United States Army

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Towards A National Strategy For Information Technology

by

Lieutenant Colonel Emanuel Hampton
United States Army

DR. Douglas V. Johnson II
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Emanuel Hampton, LTC

TITLE: Towards A National Strategy For Information Technology

FORMAT: Strategy Research Project

DATE: 7 April 1999 PAGES: 37 CLASSIFICATION: Unclassified

In the twenty-first century, our national security and our continued economic prosperity will depend on how effectively we develop national strategies and policies to shape the development and use of information technology. Specifically, how should we develop current information technologies to meet future national needs? And how do we protect current information technology infrastructures from intellectual theft, sabotage, terrorism, information warfare, and natural disasters? To maintain our current technological advantage, the United States must remain the world leader in information technologies. To remain the world leader in information technology, the United States must maintain a viable national information technology strategy.

TABLE OF CONTENTS

Information systems and networks will be to the 21st century warfighter what nuclear weapons and propulsion systems were to the 20th century warfighter.[1]

— Rear Adm. John Gauss

Our dependence on technology has made the Computer Security Technology Center's developments—electronic counterparts to guards, guns, and gates—crucial for protecting our nation's information assets.[2]

— Lawrence Livermore

THE INFORMATION TECHNOLOGY ISSUE

Rear Admiral John Gauss predicts a growing national reliance on information and other high technology systems to ensure U.S. national security in the 21st century. To maintain our nation's technological advantage, the U.S. must remain the world leader in developing leading-edge technologies. Our national security and our continued economic prosperity in the 21st century will depend on how effectively we develop national strategies and policies to control these technologies. Specifically, how should we protect our current and future technologies from theft, sabotage, terrorism, information warfare, and natural disasters? The President's Commission on Critical Infrastructure Protection (PCCIP) has recommended that we must review national policies which protect our vital infrastructures. In October 1997, the PCCIP emphatically noted new security issues caused by our entry into the era of cyber-culture:

> The United States is in the midst of a tremendous cultural change—a change that affects every aspect of our lives. The cyber dimension promotes accelerating reliance on our infrastructures and offers access to them from all over the world, blurring traditional boundaries and jurisdictions. National defense is not just about government any more, and economic security is not just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for the future security on a new form of cooperation between the private sector and the federal government.[3]

The PCCIP is right on the mark: Critical infrastructures such as cyber or information technology are key to the very survival of our nation and to the sustainment of our economic power. Our increasing dependence upon Information Technology in every key aspect of our lives has made the protection of this infrastructure paramount. However, this study reveals that the President's policies to protect our critical infrastructures are flawed. Further, we do not have a coherent national Information Technology strategy. Thus we need a comprehensive national Information Technology strategy, not the current group of uncoordinated policies.

The PCCIP listed information and communications as one of five critical national infrastructures. In this study, "Information Technologies", for the purpose of this analysis, include collection, processing, display, and communications technologies. Processing technologies include data fusion and analysis as well as support for decision making, such as "knowledge-based expert systems."[4] In my view, the most critical infrastructure is that of Information Technology. I believe that we need a viable and coherent national strategy to protect this most critical infrastructure. If we adequately protect our national Information Technology infrastructures, we will then be well on our way to resolving the challenges of the remaining four-and-a-half infrastructures: communications (and information), banking and finance, energy, physical distribution, and vital human services. The vital link to all of these infrastructures is Information Technology! Without reliable Information Technology, they are all doomed to failure! This study is divided into four related segments:

1. Review of national documents that drive our Information Technology policies.
2. Ends-ways-means analysis of IT policies to assess the soundness of these policies.
3. Discussion of future challenges that will shape and challenge our future Information Technology strategies.
4. Recommendations for a comprehensive national Information Technology strategy.

NATIONAL IT STRATEGY AND POLICY REVIEW

NATIONAL IT STRATEGY REVIEW

Two documents govern our national strategies: The President's National Security Strategy (NSS) and the National Military Strategy (NMS). The NSS specifies vital national interests, then describes economic and defense strategies to protect these vital interests. The National Military Strategy (NMS), published by the Chairman of the Joints Chief of Staff, focuses specifically on national defense. Given the recent revision of the NSS, the NMS is currently under revision.

The May 1997 NSS identifies Information Technology as an enabler for the advancement of U.S. economic and security interests. The 1997 NSS states that "Critical to our nation's ability to shape the international environment and respond to the full spectrum of crises—today and tomorrow—are technologies, capabilities and requirements to enable the continued worldwide application of U.S. national power."[5] Information Technology is cited as one of our "overarching capabilities," which include intelligence, space, missile defense, information infrastructure, and national emergency preparedness. Specifically, the United States needs accurate intelligence to support national decision-making, to identify threats, and to conduct military operations. The United States must maintain our technological edge in space to ensure our continued national security. We must enhance our missile defense systems to deter aggression. We must protect the national information infrastructures from exploitation. Finally, the United States must be prepared to respond to national emergencies, such as threats from terrorism and weapons of mass destruction.

In the October 1998 NSS revision, Information Technology was dropped from the list of overarching capabilities and apparently significantly reduced in importance. This revision cites telecommunications, energy, banking and finance, transportation, water systems, and emergency services as our key infrastructures.[6] These infrastructures are listed under the heading "Protecting Critical Infrastructures". So Information Technology is no longer a critical infrastructure-currently merely a system that sustains the operations of telecommunications, energy, banking and finance, transportation, water systems and emergency services. If information systems are essential to the operation of our critical national infrastructures, shouldn't Information Technology itself be considered a critical infrastructure? Is the 1998 NSS flawed?

The 1997 NMS advocates three strategic concepts to implement the NSS strategy: shape, respond, and prepare now. "US Armed Forces advance national security by applying military power to

Shape the international environment and **Respond** to the full spectrum of crises, while we **Prepare Now** for an uncertain future."[7] As these concepts are discussed in the NMS, Information Operations are listed as one of eight capabilities required for successful joint operations. The remaining capabilities are: decisive operations, strategic deterrence, special operations, forcible entry, force protection, countering weapons of mass destruction, and focused logistics.

Information operations are concerned primarily with the collection, processing, display, and interpretation of information. But the NMS does not include the other components of IT, telecommunications (wire, fiber, and satellite) and computer networks which support information operations. The 1997 NMS concludes that, to be successful in any operation, we must "quickly and accurately integrate critical information and deny the same to an adversary."[8] The Department of Defense will assign responsibilities at all levels to develop joint doctrine to maintain information superiority. The NMS thus clearly focuses more on information operations than on the more comprehensive category of Information Technology.

The NSS and the NMS form the foundation on which we develop our national policies. The President's Commission on Critical Infrastructures Protection (October 1997); The Department of Defense Quadrennial Defense Review (May 1997); the Institute for

National Strategic Studies, National Defense University 1998, "Strategic Assessment"; and the Army (Draft) Research, Development and Acquisition Master Plan 1999 all help define our national Information Technology policies. A brief review of these documents will enable us to further determine if we have a viable national Information Technology strategy.

NATIONAL IT POLICY REVIEW

The October 1997 report from the President's Commission on Critical Infrastructure Protection (PCCIP) identified Information Technology as one of the key national infrastructures. The PCCIP stated that the American public lacks awareness of the vulnerabilities of our critical infrastructures, noting that we take for granted that these critical infrastructures will always be available. The PCCIP also stated that there is "a need for a National Focus" and that "no one is in charge" of the protection of these key infrastructures.[9] A viable national strategy would establish a central authority—or unity of command. However, the Commission noted that "These infrastructures are so varied, and form such a large part of this nation's economic activity, that no one person or organization *can* be in charge."[10] Can we have viable Information Technology strategy with no one in charge?

The PCCIP recommended the following ways to reduce vulnerabilities to our critical infrastructures:

1. Establish Sector Coordinators to provide the focus for private industry to deal with infrastructure vulnerabilities.
2. Designate Lead Agencies within the Federal Government to implement policies.
3. Establish a National Infrastructure Assurance Council of industrial CEO's, Cabinet Secretaries, along with representatives from state and local governments, to oversee infrastructure polices.
4. Establish an Information Sharing and Analysis Center to monitor our infrastructures.
5. Establish an Infrastructure Assurance Support Office which will accommodate most of the national infrastructure policy makers.
6. Establish the Office of National Infrastructure Assurance to advise the National Security Council on infrastructure policies.

The Commission went on to assert that there is no need for "a big federal project."[11] Nonetheless, it appears they recommended a big federal project, but put no one in charge of the entire process!

Since the PCCIP's report, the President issued Presidential Decision Directive 63 (PDD 63) in May 1998: "This directive makes it U.S. Policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on our critical infrastructures, especially our information systems."[12] Two PCCIP recommendations were implemented under authority of PDD 63: The National Infrastructure Protection Center was established under the FBI as a central agency for identifying and assessing threats and conducting criminal investigations. The Critical Infrastructure Assurance Office was established under the Department of Commerce and charged with integrating the national plan to protect our infrastructures, to include the national educational program.

This security issue is also addressed in the 1997 Department of Defense (DOD) Quadrennial Defense Review (QDR). Like the NMS, the QDR acknowledges our dependency on Information Technology to meet national security objectives. Information Technology is a major enabler for the achievement of many of our national military objectives. In its assessment of the QDR, the National Defense Panel made the following observation: "In the report there is insufficient connectivity between strategy on the one hand, and force structure, operational concepts, and procurement decisions on the other."[13] The QDR begs the question of whether we can resource the necessary force structure to support our NMS: "Since 1985, America has responded to vast global changes by reducing its defense budget by some 38 percent, its force structure by 33 percent, and its procurement programs by 63 percent."[14] In view of this significant decline in military spending, can we afford to maintain adequate force structure, modernize the force, and maintain a viable IT program without significant increases of future defense budgets? Which programs will we sacrifice because of protracted under funding? Will we accept a higher risk in IT programs to maintain force structure or weapons modernization? In the final analysis, the QDR confirms that current funding is not sufficient to support our NMS. "But it has become clear that we are failing to acquire the modern technology and systems that will be essential for our forces to successfully protect our national security interests in the future"[15]

The 1998 National Defense University (NDU) "Strategic Assessment" identifies Information Technology as an enabler in shaping and projecting U.S. military forces: "Superiority in information technology enhances the other defining aspects of U.S. combat power, and its superior intelligence systems provide enough warning to enable the United States to avert or respond to crises in a timely manner without having to station forces everywhere conflict might occur."[16] Currently the United States is the world leader in the development and integration of high tech systems within its military. Specifically, Information Technology has enabled the United States to collect, process, and use information to project forces abroad and to dominate both the battlefield and the enemy.

In its discussion of Asymmetric Threats, the NDU document addresses the defensive issue of countering threats to our critical information technologies. Asymmetry refers to the "use of weapons {or technology} in ways unplanned by the United States."[17] Brigadier General (BG) Wayne M. Hall, Director of the Army's Intel XXI Project, elaborated on the concept of Asymmetrical Threats or Warfare:

> In its simplest state, Asymmetrical warfare is about *a weak opponent seeking offset against a stronger foe.* Such activity is nothing new—weaker competitors always have sought an advantage through 'offset' against a bigger, stronger foe. What is new however lies in our own vulnerabilities, our dependency on technology, our strengths being vulnerabilities, ascendancy of the digital age, advent of the information revolution, and terrorists who will be armed with weapons of mass destruction.[18]

BG Hall then identifies Information Technology as one of our centers of gravity: "That is, a place (physical or cyberspace) in which communications, collection, automation, thinking and planning merge and whose role in activities is so important that if lost, or adversely affected, would seriously jeopardize the mission."[19] If Information Technology is a Center of Gravity as BG Hall states, can we afford an unfocused strategy to protect it?

The (Draft) Army Research, Development and Acquisition Master Plan 1999 identifies six key tenets to the Army's Modernization Strategy. It references Information Technology as a key enabler in each of the tenets:

1. Gain Information Dominance: "Information dominance is the foundation for all other patterns of operation."[20] Information Dominance includes offensive and defensive operations.
2. Project the Force: The ability to rapidly deploy land power anywhere in the world. IT systems will be used to support our transportation and logistic systems.
3. Protect the Force: "The Army must protect soldiers, equipment, facilities and other crucial elements of the joint force from enemy observation and attack in all operating environments. Key elements of the digital command-and-control network [IT networks] must also be protected from electronic or information technology-based attack."[21]
4. Shape the Battle Space: "Shaping the battle space in the 21st century results from the deliberate and precise

synchronization of all combat multipliers—such as information warfare, deep attack, mobility/counter-mobility operations, and psychological operations—with a scheme of maneuver to overwhelm an adversary."[22] IT is key to the synchronization of our combat systems.

5. Conduct Decisive Operations: "The fusion of situational awareness, heightened speed and agility, enhanced lethality, and information dominance will maintain the combat overmatch currently enjoyed by Army forces."[23]
6. Sustain the Force: "No operation will succeed without focused logistics, which fuse information, logistics, and transportation technologies to deliver the right support at the right place on the battlefield at the right moment in time."[24]

The Army's Modernization Strategy is paramount to the implementation of the Army's Vision 2010 (AV2010). AV2010 describes how the Army will use current and emerging Information Technologies as combat multipliers to win future wars. Implementation and protection of Information Technologies are critical to the success of AV2010 and to building the Army After Next (AAN).

The foregoing summaries of national security documents thus serve to reveal our Information Technology policies. Are these various, overlapping national strategies and policies sufficient to maintain a viable national Information Technology infrastructure?

ENDS-WAYS-MEANS

The ends-ways-means framework undergrids Major General Richard A. Chilcoat's conception of Strategic Art:

> Strategic art entails the orchestration of all the instruments of national power to yield specific, well-defined end states. Desired end states and strategic outcomes derive from the national interests and are variously defined in terms of physical security, economic well-being and the promotion of values. Strategic art, broadly defined, is therefore: the *skillful formulation, coordination, and application of* ***ends*** *(objectives),* ***ways*** *(courses of action), and* ***means*** *(supporting resources) to promote and defend our national interests.*[25]

Accordingly, U.S. IT strategy can be described as follows:

1. The U.S. Objective (**end**) is to protect our current and emerging Information Technology infrastructures from attack, exploitation, etc.
2. The **way** we support our Information Technology objectives is through a strong focused national strategy. However, this review of pertinent documents indicates that our national IT strategy is unfocused and lacks unity of effort.

3. The U.S. has a variety of **means—or resources**—for protecting our IT infrastructure. However, we have not focused systematically on ways to use those resources. Since our IT strategy is not subject to central authority, we have no way of reliably determining whether our means are sufficient or effective.

Strategy is the vehicle (way) by which we develop national policies. National policies then govern the allocation of national resources (means) to obtain our national ends. The strategy is the glue that binds the ends to the means. A weak unformulated national Information Technology strategy simply means we will fail to protect this critical asset.

The President's Commission on Critical Infrastructure Protection has made considerable headway in identifying vulnerabilities within our critical infrastructures. Establishment of the National Infrastructure Protection Center and the Critical Infrastructure Assurance Office took us big steps in the right direction. Also the Department of Defense has made great strides in identifying Information Technology vulnerabilities and has implemented policies to reduce these vulnerabilities.

However, we still lack unity of command and unity of effort. Winn Schwartau, CEO of the Security Experts, Inc., (an international security consulting company) and the Director of

Infowar.Com (www.infowar.com), believes that the President's Commission on Critical Infrastructure Protection has been influenced by politics and is unable to provide a truly independent assessment. For example, encryption was not addressed "because it is a political hot bed right now."[26] Schwartau notes that:

> There is no mention of national leadership from the highest levels of the country. With this notable omission, I have to wonder just how much national leadership we can expect, how much political weight infowar carries, and whether this report wasn't something of a mere temporary grandstanding for a future administration to handle. Leadership is required to insure a balanced defense, complementary coordination between government and business, and carry the message forward. I haven't seen an inkling of this level of political leadership yet.[27]

We are back to the issue of "Who is in charge?" We need strong leadership both in the government and private sectors and a central authority to assure a coordinated effort from both sides. "The idea of who's in charge is left to the imagination of the reader and an unsuspecting public."[28]

The Department of Defense continues to struggle to devise effective policies to counter Information Technology vulnerabilities. Like the administration, the Department of Defense has elected not to designate a particular staff agency to oversee the protection of its critical infrastructures. In the area of Information Technology, the J6 Staff should and could take the lead. But it doesn't. I have personally observed that the J6 Staff is constantly fighting other staff agencies (such as the J3 and J4) over implementation of Information Technology policies. Further, the Air Force, Navy, Marines, and Army all have their own agendas on how Information Technology polices ought to be implemented. Within each service, there may be similar internal battles comparable to those in the Joint staff. In sum, there is no unity of effort even within the Department of Defense.

We also lack strategies and policies to support and protect Information Technology within the private sector. The Commission recommended Sector Coordinators to facilitate information sharing and cooperation with private industry. Participation would be only voluntary. Can we afford to leave the protection of our critical infrastructures on a volunteer basis? Again, we need strong leadership within the private sector to deal with such issues as: which technologies we should export or retain, how we should protect our critical technologies from theft, how we should protect critical sustaining base systems and infrastructures (such as public utilities, transportation, and banking) from sabotage and terrorist attacks, how we can control and secure the Internet, whether our technologies can be used against us, what security issues surround the year 2000 bug (Y2K) (as it pertains to national security and the private sector), how should we deal through the Internet with the world as a global village The nation has welcomed Information Technologies and already enjoyed tremendous benefits from them. But we are beginning to encounter some of the unplanned consequences of these technological advancements.

Technological advancements, especially within the Information Technology arena, have arrived much faster than we have been able to devise appropriate national strategies and policies to manage them. Current IT strategies are also inadequate because of lack of leadership, uncoordinated policies, and disunity of effort within the government and private sectors.

FUTURE CHALLENGES

We are now seriously challenged to protect Information Technology, both nationally and within the Department of Defense. "The low cost of obtaining information age technologies will help potential adversaries improve their military capabilities as they learn to leverage these technologies effectively."[29] Future adversaries will use at least five ways to challenge our information superiority: (1) They will exploit unprotected critical research and development. (2) They will exploit our military reliance on commercial services and technologies. (3) They will take advantage of our inability to unmask the anonymity of cyberspace-enemies. (4) They will exploit our inadequate redundancy in information technology systems. (5) They will exploit the rapid obsolescence of critical Information Technology infrastructures.

EXPLOITATION OF CRITICAL RESEARCH AND DEVELOPMENT (R&D)

We have failed to devise a national strategy to protect our vital Information Technology R&D efforts from theft. For example, countries such as South Korea and China pirate much of our software. In addition large quantities of software may be purchased legally on the open market or simply smuggled to unauthorized countries. Operating systems such as Microsoft Windows 95/98 are available and used heavily worldwide by both private and military organizations. Such common operating systems as Windows 95/98 may be exploited for design flaws or susceptible to viruses.

Our biggest R&D enemy may be our government! "Critics say that the administration's contradictory policies on data encryption and its slow progress on privacy controls have left the nation's nascent electronic commerce industry adrift on a rudderless ship."[30] Encryption Technology enables users to scramble data to protect electronic messages from interception or manipulation. However, the administration fears that criminals may use this technology to conceal their crimes, so the implementation of encryption software has been delayed. Encryption software is needed now to protect the consumer from fraud over the Internet. In the meantime Secretary of Commerce William Daley has admitted that "The Clinton Administration's attempts to control encryption technology have been a failure and are forcing American software makers to concede ground to foreign competitors."[31]

MILITARY RELIANCE ON COMMERCIAL SYSTEMS AND PRODUCTS

Many of the Department of Defense microcomputers and network devices are procured from commercial vendors. Our microcomputer and network design specifications are readily available to our enemies. Adversaries may study our microcomputer and network specifications to exploit design flaws. Much of our telecommunication capability, which supports our computer networks, is increasingly dependent on such commercial service providers as AT&T, MCI, and Sprint.

Commercialization or the sale of radio bandwidth is now a national security issue. "Combat sensors, communications and weapons systems require an unimpeded flow of radio frequency information that now is threatened by commercialization of the vital spectrum. The need to move more quickly than the enemy requires more wireless devices...More information moving faster requires more spectrum." The issue here is whether we will have the necessary radio bandwidth to support our IT networks[32] Colonel Alan D. Campen, USAF (Retired), currently an adjunct professor at the National Defense University claims that "More than any other country, we rely on a set of increasingly accessible and technologically reliable infrastructures, which in turn have a growing collective dependence on domestic and global networks."[33] Campen goes on to observe that "The Clinton Administration seeks to couple more closely the resources and knowledge not only of the private sector, but also its own intelligence, law enforcement and military agencies."[34] In the near future, military and private sector systems will become inseparable. What affects the private sector will also affect our military systems. Campen then offers an unfortunate judgment: "Federal proposals to forge a new national security sanctuary are impeded by ignorance, apathy, indifference, suspicion and, in some cases, determined opposition."[35] In fact, continued reliance on commercial systems will undermine our ability to function as a Joint force. "These operations (joint) depend not only on their own incompatible organic information systems, but also on the civilian owned and operated infrastructures to mobilize, transport and supply military forces."[36] Joint Vision 2010 relies on information superiority to achieve full spectrum dominance. However, our military leaders "will discover that these innovative defense strategies are hostage to civil national infrastructures."[37] Are we then to conclude that Joint Vision 2010 is seriously flawed because of its over-reliance on commercial products and systems, specifically commercial information infrastructures? Have we truly put all our eggs in someone else's basket? According to some analysts, we have already done this: " Moreover DOD's increasing reliance on COTS [Commercial Off The Shelf] hardware and software increases vulnerabilities by making military systems familiar to sophisticated adversaries and by exposing them to software developers and technicians who are not subject to security regulations. Hence, design and acquisitions procedures need to consider security and minimize exposure. Indeed, some systems may be too sensitive to rely on COTS design or procurements."[38]

ANONYMITY OF CYBER-ENEMIES

DOD computers and computer systems have already been attacked over 250,000 times. Sixty-five percent of these were estimated to be successful.[39] The number of attacks is estimated to be doubling each year. During the Cold War, the enemy was more identifiable. However, the face of future enemies will not be so easily identified. A potential terrorist can attack our information systems by inserting a virus from anywhere in the world without leaving a trace. Our "enemy" may be a bored high school student who hacks our information system for entertainment. Personnel employed in high tech areas will continue to change employers for better opportunities; some may even choose to work for an international corporation. Where will their loyalties lie, with the nation or with the international corporation? According to a survey of Fortune 1000 Corporations, "Nearly half of the 205 firms that responded admitted that their computer networks had been successfully attacked and penetrated by 'outsiders' in the past year--with losses and associated costs considerably higher than previously estimated."[40] How do we protect our human knowledge from such exportation or exploitation?

It is estimated that the Department of Defense has 2.1 million computers and 10,000 local area networks.[41] These systems are used for intelligence, solider support, logistics, and mobilization efforts. In fact these information systems provide "the very basis of our war-fighting capability."[42] These systems are vulnerable to many of the new Weapons of Information Warfare such as:

1. Malicious software such as viruses—there are between 9,000 to 12,000 known viruses.
2. Chipping—the process of changing the functions of microchips.

3. Van Eck—the process which allows one to monitor radio emissions from electronic devices.

4. Spoofing—the ability to fake a legitimate user.[43]

Terrorists, hostile nations, and cyber-criminals may attack our vital commercial and defense information systems using weapons of information warfare.

The private sector is even more susceptible to cyber-criminals, especially from corporate insiders. "Insiders have the advantage of not needing to break into computer systems from the outside, but only to use, or abuse, their legitimate access."[44] Former employees who perceive themselves as having been wronged by the corporation may be our new cyber-criminals. These disgruntled former employees are hard to trace because they have "intimate knowledge of where the most sensitive information is stored, how to access the information, and how to steal or damage the data."[45]

REDUNDANCY

What can we do when parts of our telecommunication systems are rendered helpless by a power blackout caused by a natural disaster? "For example, electric power grids and natural gas pipelines are controlled by computer systems."[46] The backbone of our information and communication networks is provided through commercial service providers such as AT&T, MCI, and Sprint. Can we sufficiently off-route critical information systems during a national emergency? During a crisis, can we afford to wait three days for the restoration of basic services, as occurred during Hurricane George (1998)? Much of the national utility infrastructure is above ground, easily vulnerable to natural disasters and terrorist attacks. Will we be able to transition to manual systems? Banks rely totally on automated systems. Ledger books are a thing of the past. Wall Street is highly dependent on automation systems and would be hard pressed to replace these automation systems during a sustained outage. However, they are working on these critical issues. "The year 2000 computer problem and several related factors could trigger a worldwide economic decline in 1999-2001"according to a professor of finance.[47] Will we be able to make critical decisions when our intelligence systems become inoperable? In the future, many of the telecommunications networks that support our IT infrastructures will be dependent upon foreign operated or multinational operated infrastructures. Such dependence will further reduce our ability to provide redundancy and restoration of critical infrastructures during a crisis. As we demand faster and more reliable information, our infrastructures will be pushed to the maximum to meet this demand at the expense of redundancy. Our national strategy must address the problem of redundancy in our most critical infrastructures. We must plan nationally for the immediate restoration of critical infrastructures during a crisis. "Increased reliance on high-tech systems for information collection, interpretation, processing, analysis, communications, and display has made failures in these systems more disruptive."[48]

OBSOLESCENCE

"Information Technology doubles roughly every one and a half to three years. Each successive generation is both faster but cheaper, smaller, and less power-hungry as well."[49] Other critical infrastructures are probably wrestling with similar problems of obsolescence. As we plan today for the military of 2010, are we procuring technologies that may be outdated before 2010? How should we allocate funds within the military for timely replacement of aging systems? Is current national strategy to modernize our current infrastructures, such as power and telecommunications, adequate? The operating speed of a 350mhz processor vice a 300mhz processor may provide the difference that wins the next war! The Chinese have learned to play the game of modernization. They recognize that "...it seems that the further technology develops, the easier it becomes to catch up."[50] We may be spending billions of dollars today to implement Joint Vision 2010; the Chinese may spend a few million of dollars to buy a better and cheaper technology tomorrow. Our old foe Iraq may acquire technologies in the year 2010 that rival our military capabilities, thereby eliminating our technological edge during Desert Storm! If we sink too much today in IT, we may be obsolete tomorrow. On the other hand, can we afford to take the risk of waiting for future technologies?

Our current national strategies simply do not meet the coming challenges to Information Technology. "Given that our potential adversaries have access to virtually the same information technologies that we have, the margin for victory will be the degree to which we manage our transformation into the information age."[51]

RECOMMENDATIONS

Our overall national security can be successful only if our critical infrastructures are protected. The following recommendations will contribute to a viable Information Technology strategy:

1. The President must establish a cabinet level position to oversee our critical infrastructures (a proposal rejected by the PCCIP). This position, The Secretary of Critical Infrastructures (SCI), will develop integrate and monitor compliance with a comprehensive national strategy for dealing with our national infrastructures.

2. The President must establish the Department of Critical Infrastructures (DCI) under the Secretary of Critical Infrastructures. For starters, move the Critical Infrastructures Assurance Office from the Department of Commerce to the Department of Critical Infrastructures and consider putting the National Infrastructure Assurance Office, which is currently under the FBI, under the operational control of the Department of Critical Infrastructures.
3. The DCI must develop a strong, comprehensive national Information Technology strategy. This strategy must provide a coordinated national strategy, unifying concerns and efforts of both government and private sectors. It must seek to identify unintended effects of new Information Technologies, take advantage of unexpected opportunities, and keep pace with emerging technologies.[52]
4. The SCI must persuade Congress to continue to enact legislation that protects our vital military and private Information Technologies from potential enemies and competitors. Congress must also enact legislation to encourage the private sector to conduct vital Research and Development. The SCI must devise ways to protect our intellectual property.

5. The Department of Education must develop programs that ensure the continued supply of future IT professionals, who will support ongoing development of our critical infrastructures.

6. The Department of State must ensure that the status of "Most Favored Nation" is granted only to countries that observe our copyright laws. It must further ensure that intellectual property rights are protected through the United Nations and other international organizations.

7. The SCI must have the authority to enforce laws governing critical infrastructures.

8. The Department of Defense should consider establishing an Information Corps. "Technology, used correctly, begets doctrine; doctrine begets organization."[53] As a Joint Corps, the Information Corps would be responsible for identifying critical Information Technologies, developing joint doctrine, prioritizing acquisition, ensuring interoperability between the services, and the protecting of critical information infrastructures within the Department of Defense.[54] Only such a joint effort will provide a sound, secure, state-of-the-art Information Technology Infrastructure within the Department of Defense. "To the extent that tomorrow's military power is defined by expertise at information rather than the application of

force, military superiority may flow to those organized for the former task rather than the latter one."[55]

CONCLUSION

There is little doubt that the sustainment of our technological edge in the area of Information Technology is critical to our continued economic well-being and national survival. Information Technology has been a major contributor to our superpower status, world economic dominance, and military might as demonstrated during the Persian Gulf War. In the past the United States has employed technology that our competitors and enemies did not have. We have demonstrated to the world the advantages of information technology as an economic advantage and military force multiplier. The world has taken notice. We must now implement a comprehensive national strategy to ensure that we maintain our edge in information technology!

> **Top Defense Department information officers believe that information technology and computerized weapons will determine winners and losers of future battles.**[56]
>
> **— Bob Brewin**

> **There are no simple answers but one thing is certain. Any nation which ignores the threat of IW (Information Warfare) attacks may one-day face an electronic equivalent of the 1941 attack on Pearl Harbor.**[57]
>
> **— Doug Richardson**

Word Count 5,721

ENDNOTES

[1] Bob Brewin, "Software, IT as vital to military as ships, tanks," Federal Computer Week, (27 April 1998): 14.

[2] Lawrence Livermore, " Making Information Safe"," Science & Technology Review, (January/February 1998):4.

[3] The President's Commission on Critical Infrastructures Protection, Critical Foundations, Thinking Differently, report prepared by The President's Commission on Critical Infrastructure Protection, (October 1997):1.

[4] David S. Aberts, The Unintended Consequences of Information Age Technologies, (Washington, D.C.: The Center for Advanced Concepts and Technology, National Defense University, 1996), 15.

[5] The White House, A National Security Strategy For A New Century, (May 1997): 13.

[6] The White House, A National Security Strategy For A New Century, (October 1998): 20.

[7] Chairman of the Joints Chief of Staff, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era, (1997): 11.

[8] Ibid., 27.

[9] The President's Commission on Critical Infrastructures Protection, 5.

[10] Ibid.

[11] Ibid.

[12] The White House, A National Security Strategy For A New Century, (October 1998): 20.

[13] National Defense Panel, " Assessment of the May 1997 Quadrennial Defense Review, " 9 October 1998, available from < http://www.defenselink.mil/topstory/ndp assess.html >.Internet.Accessed 9 October 1998.

[14] William S. Cohen, Report of the Quadrennial Defense Review, Joint Forces Quarterly, (summer 1997):8.

[15] Ibid.

[16] National Defense University, 1998 Strategic Assessment Engaging Power for Peace, Institute for National Strategic Studies (Washington D.C.: National Defense University, March 1998), 33.

[17] Ibid., 169.

[18] Brigadier General Wayne M. Hall, " Thoughts on Meaning of Asymmetrical and Asynchronous Threats in the 21st Century" (Unpublished Paper): 1.

[19] Ibid., 5

[20] Department of Army, " Research, Development and Acquisition Draft Master Plan," (Washington, D.C.: U.S. Department of the Army, 1998), 8.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Richard A. Chilcoat, "Strategic Art: The New Discipline for the 21st Century Leaders," in USAWC, Selected Readings: Course 1 Strategic Leadership, Volume I (USAWC 1998), 85.

[26] Winn Schwartau, "Thoughts on the PCCIP Report" available from betty@infowar.com, 22 October 1996, 3.

[27] Ibid., 5.

[28] Ibid.

[29] Alberts, 10.

[30] Jeri Clausing, "Critics Question U.S. Policy on Electronic Commerce", available from jeri@nytimes.com, 15 June 1998, 1.

[31] Jeri Clausing, "Commerce Chief Calls U.S. Encryption Policy Flawed", available from jeri@nytimes.com, 16 April 1998, 1.

[32] "Army Information Experts Seek Commercial Solutions" Signal (June 1998): 45.

[33] Alan D. Campen " National Vulnerability Intensifies As Infrastructure Reliance Grows" Signal(July 1998): 20.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Alberts, 41.

[39] Major Keith D. Anthony, "Information Warfare: Good News and Bad News," Military Intelligence, (January-March 1997):31.

[40] Steve Shaker, "1996 Information Systems Security Survey", 11 November 1996. Available from < http://www.warroomresearch.com/WRR/SurveysStudies/961121 96ISSSurvey.htm >; Internet; accessed 16 October 1998:1.

[41] Anthony, 31.

[42] Ibid.

[43] Ibid., 33.

[44] Michael A. Vatis, " Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record," 24 March 1998; available from http://www.fbi.gov/images; Internet; accessed 17 October 1998:4.

[45] Ibid.

[46] Ibid.,2.

[47] Quoted by Russ Ray, "What the Year 2000 Problem May Do to the Stock Market and the Economy," The Futurist, (August-September 1998):16.

[48] Alberts, 18.

[49] Martin C. Libicki, "The Mess And The Net, " National Defense University, March 1994, 7.

[50] Anthony, 32.

[51] Alberts, 7.

[52] Ibid., 11.

[53] Libicki, 50.

[54] Ibid.

[55] Alberts, 11.

[56] Berwin, 14.

[57] Doug Richardson, " Information Warfare —New Threats And New Opportunities" Asian Defense Journal, (April 1997): 51.

BIBLIOGRAPHY

A National Security Strategy For A New Century, report prepared by the White House, May 1997, 13.

A National Security Strategy For A New Century, report prepared by the White House, October 1998, 20.

Alberts, David S. The Unintended Consequences of Information Age Technologies. Washington, D.C.:The Center for Advance Concepts and Technology, National Defense University, 1996.

Anthony, Keith D. " Information Warefare: Good News and Bad News." Military Intelligence (January-March 1997): 31.

Antal, John F. "Battleshock 21 A Future History." United States Army.

"Army Information Experts Seek Commercial Solutions." Signal (July 1998): 45.

Assessment of the May 1997 Quadrennial Defense Review, National Defense Panel, 9 October 1998. Available from <http://www.defenselink.mil/topstory/ndp assess.html>. Internet. Accessed 9 October 1998.

Atkinson, Rick. "Crusade." Boston, MA.: Houghton Mifflin Company, 1993.

Brewin, Bob. "Software, IT as vital to military as ships, tanks." Federal Computer Week, 27 April 1998, 14.

Campen, Alan D. "National Vulnerability Intensifies As Infrastructure Reliance Grows." Signal (July 1998): 20.

Childcoat, Richard A. " Strategic Art: The New Discipline for the 21st Century Leaders." In USAWC, Selected Readings: Course 1, Strategic Leadership, 1998, Volume 1, 85.

Clausing, Jeri. "Commerce Chief Calls U.S. Encryption policy Flawed." Available from jeri@nytimes.com. 15 June 1998.

Clausing, Jeri. "Critics Question U.S. Policy on Electronic Commerce." Available from jeri@nytimes.com. 16 April 1998.

Coale, John C. "Fighting Cybercrime." Military Review (March-April 1998): 78.

Cohen, William S. "Report of the Quadrennial Defense Review." Joint Forces Quarterly, Summer 1997, 8.

Critical Foundations, Thinking Differently, report prepared by The President's Commission on Critical Infrastructures, President's Commission on Critical Infrastructures, October 1997, 1.

Gumbert, Jack. "Leadership in the Digitized Force." Military Review, (January-February 1998):13.

Hall, Wayne M. "Thoughts on Meaning of Asymmetrical and Asynchronous Threats in the 21st Century". Unpublished Paper.

Hoo, Kevin S, Seymour Goodman, and Lawrence Greenberg. " Information Technology and the Terrorist Threat." Survival (Autumn 1997),vol.39, no.3, 135-55.

Kevles, Daniel J. " Science in Transition: Searching for a Role in the Post-Cold War Era." USA Today (September 1998):25.

Laqueur, Walter. "The New Face of Terrorism." The Washington Quarterly (Autumn 1998): 169.

Libicki, Martin C. "The Mess And The Net." Washington, D.C., National Defense University, March 1994.

Livermore, Lawrence. "Making Information Safe." Science & Technology Review, January/February 1998, 4.

Lyman, Isabel. " What's Behind the Growth in Home Schooling?" USA Today (September 1998): 64.

Mann, Charles C. "Who Will Own Your Next Good Idea?" The Atlantic Monthly, (September 1998): 57.

Meinel, Carolyn P. " How Hackers Break In…and How They Are Caught." Scientific American (October 1998): 98.

Murray, Williamson. "Clausewitz Out, Computer In." The National Interest (Summer 1997): 57.

National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Area. Washington, D.C.: Chairman Joint Chiefs of Staff, 1997, 11.

Peterson, John L. "The Road to 2010" Corte Madera, CA.:Waite Group Press, 1994.

Ray, Russ. "What the Year 2000 Problem May Do to the Stock Market and the Economy." The Futurist, (August-September 1998): 16.

Richardson, Doug. "Information Wareface-New Threats And New Opportunities." Asian Defense Journal, (April 1997):51.

Rivest, Ronald L. " The Case against Regulating Encryption Technology." Scientific American (October 1998): 116.

Schwartau, Winn. " Thoughts on the PCCIP Report." 1996. Available from betty@infowar.com; Internet.Accessed 22 October 1996.

Shaker, Steve. "1996 Information Systems Security Survey." 11 Novemeber 1996. Available from http://WWW.warroomresearch.com/WRR/SurveysStudies/961121 96ISSSurvey.htm. Internet.Accessed 16 October 1998.

Strategic Assessment Engaging Power for Peace. Washington, D.C.: Institute for National Strategic Studies, National Defense University, March 1998, 33.

U.S. Department of the Army. Research, Development and Acquisition Draft Master Plan. Washington, D.C: U.S. Department of the Army, 1988.

Vatis, Michael A. " Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record." 24 March 1998. Available from <http://www.fbi.gov/images. Internet.Accessed 17 October 1998.

Zimmermann, Philip R. "Cryptography for the Internet." Scientific American (October 1998): 110.